Redacción de Informe Técnico Completo sobre una Vulnerabilidad Confirmada

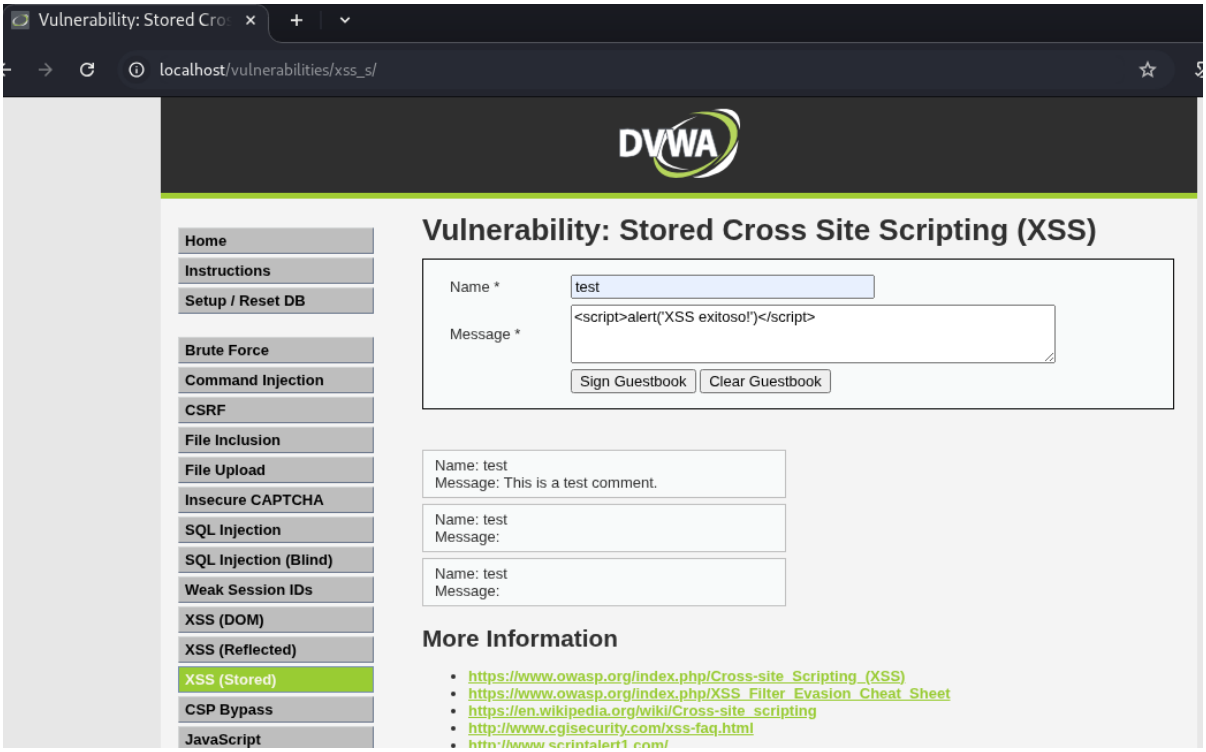
1. Descripción

Se ha identificado una vulnerabilidad de tipo XSS Almacenado en el campo de comentarios (guestbook) del módulo "XSS (Stored)" de la aplicación web DVWA. Esta falla permite a un atacante inyectar y almacenar código malicioso en la base de datos de la aplicación. Dicho código se ejecuta automáticamente en el navegador de cualquier usuario que acceda a la página afectada, sin necesidad de interacción adicional.

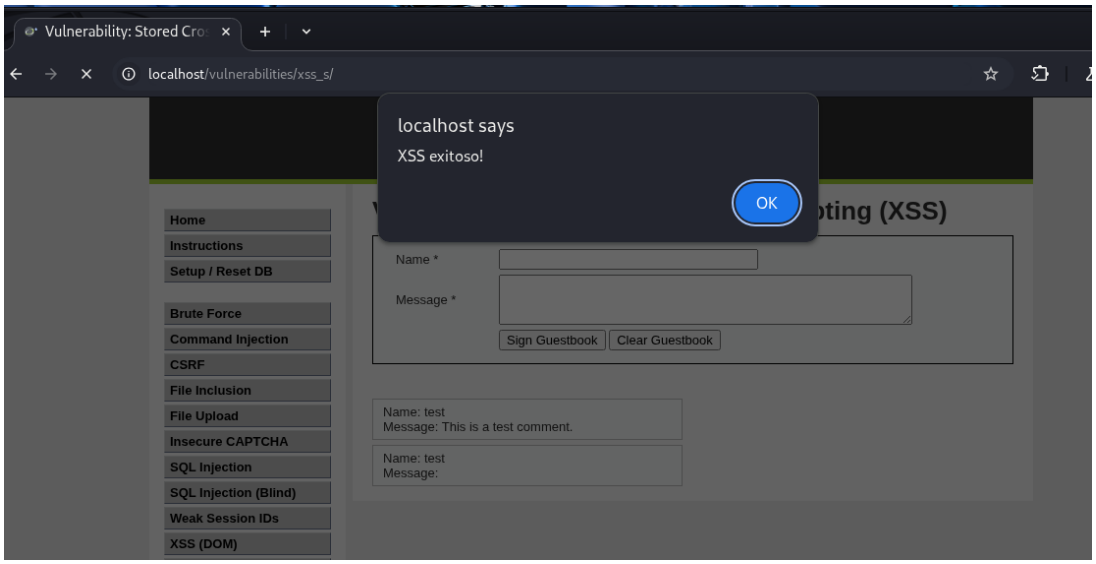
2. Evidencia Técnica

- **Payload utilizado**: Se inyectó el siguiente código JavaScript en el campo de comentarios de la aplicación.

<script>alert('XSS exitoso!')</script>



- **Comportamiento del sistema**: Al ingresar el payload y enviar el formulario, la aplicación web almacenó el código. Posteriormente, al recargar la página, el navegador del usuario lo interpretó como código válido, ejecutando el comando alert() y mostrando una ventana emergente. Esto demuestra que la aplicación no sanitiza ni escapa correctamente la entrada del usuario, permitiendo la ejecución de scripts maliciosos.



  - **Pasos de reproducción**:
    - Navega al módulo "XSS (Stored)" en la aplicación DVWA con el nivel de seguridad configurado en Low.
    - En el campo de comentarios, ingresa el payload <script>alert('XSS exitoso!')</script>.
    - Haz clic en el botón "Sign Guestbook" para enviar los datos.
    - El navegador ejecutará el script, y aparecerá una ventana emergente que confirma la vulnerabilidad.

3. Evaluación de Impacto y Riesgo

- **Impacto**: La vulnerabilidad tiene un impacto significativo porque el payload malicioso se almacena de forma persistente. Un atacante podría robar cookies de sesión de otros usuarios, comprometer credenciales, o realizar acciones no autorizadas en nombre de los usuarios legítimos.
- **Riesgo**: El riesgo de esta vulnerabilidad se clasifica como **Alto**. La explotación es sencilla y el impacto potencial puede comprometer a toda la base de usuarios y la seguridad de la aplicación.

4. Recomendaciones Técnicas

Para mitigar esta vulnerabilidad, se recomienda implementar las siguientes medidas de seguridad:

- **Validación de Entrada**: La aplicación debe validar y filtrar todos los datos de entrada, utilizando listas blancas para permitir solo caracteres esperados y no permitir etiquetas HTML, scripts o cualquier otro contenido malicioso.
- **Escapado de Salida (Output Encoding)**: Es fundamental codificar todo el contenido que se muestra en el navegador, asegurando que los caracteres como < y > sean escapados como < y >.
- **Content Security Policy (CSP)**: Se recomienda implementar una cabecera CSP para restringir las fuentes de contenido que el navegador puede cargar, evitando la inyección de scripts desde fuentes externas.

5. Reflexión Final

- **Diferencia entre informe y alerta**: Un informe profesional se diferencia de una simple alerta técnica al proporcionar un análisis completo de la vulnerabilidad, incluyendo su impacto, riesgo y recomendaciones concretas para su mitigación.
- **Importancia del lenguaje**: La estructura y el lenguaje técnico en un reporte de seguridad son cruciales para comunicar de manera efectiva el riesgo a los equipos de desarrollo y la gerencia, facilitando la toma de decisiones informadas para solucionar el problema.